УДК 004.41

Н.С.МОГИЛЕВСКАЯ, В.Р.СКОРОБОГАТ, В.С.ЧУДАКОВ

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ДЕКОДЕРОВ КОДОВ РИДА-МАЛЛЕРА ВТОРОГО ПОРЯДКА

Представлены результаты сравнительных экспериментов по исследованию корректирующей способности двух вероятностных декодеров кодов Рида-Маллера (декодер Сидельникова-Першакова и декодер Лоидрю-Саккура). Для получения результатов экспериментов программно реализована имитационная модель цифрового канала передачи данных.
Ключевые слова: *коды Рида-Маллера, вероятностный декодер, экспериментальное исследование декодеров.*

Введение. В настоящее время одной из актуальных задач техники связи является построение новых алгоритмов декодирования известных помехоустойчивых кодов. Основной целью их построения является нахождение и исследование таких методов непереборного декодирования, которые по своим характеристикам были бы по возможности близкими по эффективности к переборным алгоритмам и при этом сохраняли бы приемлемое значение оценки сложности.

Сейчас активно разрабатываются новые декодеры и для давно известных и хорошо изученных кодов Рида-Маллера (код РМ). Напомним, что коды РМ являются простейшим примером класса геометрических кодов. Параметрами этих кодов является пара натуральных чисел m и r, r**<**m. Характеристики кода РМ: длина $n=2^m$; размерность $k = C_m^0 + C_m^1 + \ldots + C_m^r$, минимальное кодовое расстояние $d = 2^{m-r}$, количество гарантированно исправляемых ошибок $t = 2^{m-r-1} - 1$. Коды РМ с параметрами m,r далее будем обозначать РМ(r,m). В случае r=2 коды РМ принято называть кодами второго порядка. Сложность алгоритма декодирования полным перебором пропорциональна числу элементов кода и даже для кода РМ второго порядка имеет не полиномиальную функцию оценки сложности [1].

За последнее время предложен ряд новых декодеров кодов РМ. Так, в работах [2-6] предложены мягкие декодеры кодов РМ, особенность которых заключается в том, что алгоритм получает на вход, возможно, искаженное кодовое слово, координаты которого записаны вещественными числами. Эта особенность позволяет объединять такие алгоритмы в каналах связи с демодуляторами. Представленный в работе [2] алгоритм мягкого декодирования кодов Рида-Маллера имеет сложность порядка $n\ln n$ и позволяет исправлять большинство ошибок веса $\sqrt{n/\ln n}$. В работе [7] представлен списочный декодер, особенностью которого является то, что на выходе алгоритма вычисляется не одно кодовое слово, а список наиболее вероятных кодовых слов, при этом длина списка определяется параметрами алгоритма.

В работах [8-10] предложены вероятностные алгоритмы декодирования кодов РМ. Особенностью вероятностных алгоритмов является возможность с большой вероятностью корректировать кодовые слова, ошибки в которых превышают число t гарантированно исправляемых ошибок.

Постановка задачи. В данной работе необходимо провести сравнительное исследование мажоритарного декодера (МД) [1], вероятностного декодера Сидельникова-Першакова (СПД) [8] и модифицированного декодера Сидельникова-Першакова (МСПД) [10] кодов Рида-Маллера. Для проведения экспериментов необходимо программно реализовать указанные алгоритмы декодирования.

Далее рассмотрим особенности используемых алгоритмов декодирования и сведения об их программной реализации. Укажем условия проводимых экспериментов и их результаты.

Мажоритарный декодер кода Рида-Маллера. Был предложен Ридом в 50-х годах XX века. Алгоритм позволяет гарантированно исправлять все ошибки веса, не превышающего t. Отметим, что алгоритм декодирования Рида восстанавливает сразу информационное слово, не находя соответствующего ему верного кодового слова. Восстановление информационного слова ведется итерационно по r блокам порождающей матрицы кода РМ, начиная с нижнего. На каждой итерации восстанавливаются биты информационного слова, соответствующие текущему блоку с помощью вычисления специальным образом подобранных контрольных сумм и мажоритарного голосования.

Декодер Сидельникова-Першакова. В работе [8] авторами предложен вероятностный алгоритм декодирования кодов Рида-Маллера второго и третьего порядка при числе ошибок, превышающем значение t. СПД рассматривает проблему декодирования кодового слова РМ(2,m) кода как задачу декодирования n кодовых слов РМ(1,m) кода. Этот алгоритм параметризуется двумя целыми значениями s и h, где $s \in [1,..,n]$, $h \geq 0$, которые отвечают за глубину перебора при поиске верных значений на одном из этапов алгоритма. Согласно [8] этот алгоритм имеет сложность порядка $n^2(m + hs^3)$ и позволяет почти всегда исправлять ошибки веса $t - (n \quad Cm^{1/4}n^{3/4})/2$ при $m \to \quad , C > \ln 4$.

Модифицированный декодер Сидельникова-Першакова. Авторами работ [9, 10] предложена модификация СПД, которая, по мнению авторов, обеспечит декодирование большего числа ошибок по сравнению с оригинальным декодером из [8]. Кратко рассмотрим идею модификации СПД. Так, в алгоритме, разработанным Лоидрю и Саккуром, параметры s и h отсутствуют, и поиск ведется с фиксированным параметром s=1. Помимо этого в алгоритме отсутствуют действия, уточняющие значения и управляемые параметром h, но добавлено отсутствующее в СПД мажоритарное голосование, уточняющее элементы массива, содержащего данные о части информационного слова, стоящей при квадратичной составляющей кодирующей булевой функции [10]. Такое уточнение элементов массива происходит на третьем шаге алгоритма МСПД, далее при необходимости сослаться на этот шаг будем называть его «уточняющим шагом». Согласно [9], модифицированный алгоритм имеет сложность $n^2 \log(n)$ и позволяет исправлять $n/2(1 - \varepsilon)$ ошибок, где ε превышает величину $n^{-1/3}$.

Программное средство. Все рассмотренные декодеры кодов РМ – МД, СПД, МСПД были программно реализованы на языке СИ++ в среде MS Visual Studio 2005 и Borland C++ Builder. Построенная программная реализация позволяет применять мажоритарный декодер к кодам РМ любого порядка

до десятого включительно. Для возможности исследования влияния уточняющего шага МСПД на работу алгоритма в программном средстве была реализована возможность не выполнять этот шаг, а при необходимости заменять его шагом-«заглушкой», сохраняющим массив уточняемых данных без изменений.

Для проведения экспериментов построена программная утилита, позволяющая накладывать на правильные кодовые слова вектора ошибок заданного веса. Моделируемые вектора ошибок считаются поступающими из стационарного двоичного симметричного канала без памяти и без стираний и действуют на кодовые слова аддитивно [11].

Методика проведения экспериментов. Схема проведения экспериментов аналогична схеме, предложенной в работе [8]. А именно, для кода РМ с фиксированными параметрами случайным образом генерируется некоторое информационное слово и вычисляется соответствующее ему правильное кодовое слово, на которое накладывается случайный вектор ошибок заданного веса. Искаженное кодовое слово поступает на вход алгоритма декодирования. Результат декодирования сравнивается с правильным информационным словом, если эти вектора совпадают, то выносится решение об успешном декодировании, иначе декодирование считается неверным. Для фиксированных параметров кода РМ и каждого алгоритма декодирования (в случае СПД и для каждой фиксированной пары параметров s и h) такие испытания проводились 1000 раз.

Результаты работы декодеров приведены в табл.1. Опишем структуру этой таблицы. В первом столбце находится параметр m исследуемого кода Рида-Маллера второго порядка (параметр r фиксируется, r=2), а также для удобства приведены параметры: n и k – длина и размерность кода, t – расчетное значение числа гарантированно исправляемых ошибок. Во втором столбце записан вес случайного вектора ошибок, накладываемого на правильное кодовое слово. Третий и пятый столбцы содержат процент правильно декодированных кодовых слов мажоритарным декодером и декодером Сидельникова-Першакова, соответственно. Параметры s и h, использованные в декодере Сидельникова-Першакова, указаны в четвертом столбце. Шестой и седьмой столбцы содержат результаты, полученные с применением модифицированного декодера Сидельникова-Першакова, при этом в шестом столбце указаны результаты работы декодера, описанного в [12, 13], а в седьмом столбце указаны результаты, полученные этим же декодером без использования его уточняющего шага.

Таблица 1

Результаты экспериментов по исследованию
эффективности декодеров кодов Рида-Маллера второго порядка

Параметры кода, m, n, k, t	$W_H(e)$	МД, %	s, h	СПД, %	МСПД, %	МСПД без уточняющего шага, %
1	2	3	4	5	6	7
5, 32, 16, 3	3	100	1, 3	100	100	100
	4	2,6	1, 3	23	20,7	19
	4		3, 1	28		
	5	0,7	1, 0	6,9	8,6	3,7
	5		1, 3	10,1		
	5		3, 1	10,3		

Окончание табл.1

1	2	3	4	5	6	7
6, 64, 22, 7	7	100	1, 3	100	100	100
	11	1,3	1, 3	64,6	62,8	48,6
	11		3, 1	68,1		
	11		3, 3	67,2		
	13	0	3, 1	5,4	9,7	0,1
	13		1, 3	4,7		
	13		3, 3	7		
7, 128, 29, 15	15	100	1, 3	100	100	100
	29	0	1, 3	52,2	48,1	3,1
	29		3, 1	61,3		
	29		3, 3	66,4		
	30	0	3, 1	29,1	32,3	0,4
	30		1, 3	38,7		
	30		3, 3	42,1		
8, 256, 37, 31	31	100	1, 3	100	100	100
	69	0	1, 3	67,8	77	14,2
	69		3, 1	75,4		
	69		3, 3	81,2		
	72	0	1, 3	10,1	56,2	1,7
	72		3, 1	21,3		
	72		3, 3	35,7		
	73	0	1, 3	3,2	41,6	0,8
	73		3, 1	8,3		
	73		3, 3	18,6		
9, 512, 46, 63	63	100	1, 3	100	100	100
	159	0	1, 3	52,2	96	9
	159		3, 1	80,6		
	159		3, 3	92,2		
	164	0	1, 3	1,4	76,2	0
	164		3, 1	10,4		
	164		3, 3	31,8		

Для оценки времени работы уточняющего шага алгоритма МСПД подсчитано количество арифметических операций и операций присвоения в конкретной программной реализации для значений m=7 и m=9.

Таблица 2

Сравнение количества арифметических операций и операций присвоения алгоритмов МСПД и МСПД без уточняющего шага

Параметры алгоритма	Количество арифмет. операций		Количество операций присвоения	
	m=7 (n=128)	**m=9 (n=512)**	**m=7 (n=128)**	**m=9 (n=512)**
Алг. МСПД	34 992 847	2 641 687 827	18 529 932	1 384 989 044
Алг. МСПД без уточняющего шага	34 750 912	2 636 726 528	18 287 996	1 380 027 744
Различие, %	0,69	0,19	1,31	0,36

Обсуждение результатов экспериментов

1. Анализ значений, приведенных в табл.1, показал, что мажоритарный декодер, как и ожидалось, полностью исправляет все ошибки в кодовых словах, в случае, если количество ошибок не превышает числа гарантированно исправляемых ошибок t; при числе ошибок, превышающем значение t, мажоритарный декодер практически не исправляет ошибки.

Вероятностные алгоритмы также показали стопроцентное исправление ошибок при числе ошибок, не превышающем t, однако при увеличении значения t не происходит такого лавинообразного уменьшения правильно декодированных слов, как при мажоритарном декодировании.

2. Результаты работы программной реализации алгоритма Сидельникова-Першакова совпадают с результатами, представленными его авторами в работе [8], что подтверждает корректность работы, построенной программной реализации.

3. При увеличении значений параметров s и h СПД происходит увеличение числа правильно декодированных слов. Эксперименты показали, что наиболее значимым является параметр s. Отметим также, что увеличение параметра h приводит к значительному возрастанию времени работы программы.

4. При параметрах s=1 и h=0 время работы алгоритма СПД практически совпадает со временем работы алгоритма МСПД. При увеличении значений s и h алгоритм СПД работает медленнее алгоритма МСПД.

5. Алгоритм МСПД без применения уточняющего шага показывает результаты схожие с результатами алгоритма СПД с параметрами s=1 и h=0. Применение уточняющего шага алгоритма МСПД существенно увеличивает вероятность правильного декодирования кодового слова. При этом, согласно табл. 2, влияние уточняющего шага на время работы приложения практически не значимо.

6. Выгода от использования МСПД возрастает с увеличением значения m. С увеличением параметров s и h алгоритма СПД эффективность декодирования увеличивается, но при этом не превосходит некоторого порогового значения, так, например, при m>8 даже со значениями параметров s и h, приближающимися к значению 10, СПД обладает меньшей корректирующей способностью по сравнению с алгоритмом МСПД.

7. Более детальный анализ результатов проведенных экспериментов показал, что исследуемые алгоритмы практически не чувствительны к местоположению ошибок внутри кодового слова.

Выводы. Реализованные алгоритмы СПД и МСПД позволяют эффективно восстанавливать кодовые слова, искаженные ошибками, число которых превышает t. Как показали эксперименты, выбор одного из этих декодеров должен определяться задачами, возникающими на практике. А именно, алгоритм СПД позволяет гибко варьировать эффективность декодирования с помощью параметров s и h, при этом существенно меняя время работы алгоритма. Алгоритм МСПД в случаях при m>7 позволяет корректировать большее число ошибки, по сравнению с алгоритмом СПД.

В рассмотренных вероятностных алгоритмах декодирования кодов РМ присутствовали шаги, на которых необходимо случайным образом выбрать одно значение из некоторого множества, при этом выбор того или иного значения влияет на результат декодирования. Если в таких ситуациях выбирать не одно значение из множества равных, а запоминать и использовать в процессе декодирования их все, то на выходе алгоритма декодирования будет создан список кодовых слов. С учетом этой особенности в дальнейшем нами планируется модификация алгоритма МСПД на случай списочного декодирования.

Библиографический список

1. *Мак-Вильямс Дж.* Теория кодов, исправляющих ошибки / Дж.Мак-Вильямс, Дж.Слоен. – М.: Связь, 1979. – 744 с.
2. *Dumer I.* Soft-decision decoding of Reed-Muller codes: A simplified algorithm, IEEE transactions on information theory, vol. 52, no. 3, March 2006. – Pp. 954-963.
3. *Solte N., Sorger U.* Soft-decision stack decoding of binary Reed-Muller codes with "Look-ahead" technique. 7th International Workshop on Algebraic and Combinatorial Coding Theory, pp. 293-298, Bansko, Bulgaria, 18-24 June 2000.
4. *Ashikhmin A., Litsyn S.* Simple MAP decoding of first-order Reed-Muller and Hamming codes, IEEE transactions on information theory, vol. 50, no. 8. –August 2004. – Pp. 1812-1818.
5. *Schnabl G., Bossert M.* Soft-Decision decoding of Reed-Muller codes as generalized multiple concatenated codes, IEEE transactions on information theory, vol.41, no. 1. – January 1995. – Pp. 304-308.
6. *Lucas R., Bossert M., Dammann A.* Improved soft-decision decoding of Reed-Muller codes as generalized multiple concatenated codes, Proc. ITG Conf. source and channel coding, Aahen. - Germany, 1998. – Pp. 137-141.
7. *Dumer I., Shabunov K.* Soft-decision decoding of Reed-Muller codes: Recursive lists, IEEE Transactions on information theory, vol. 52, no. 3, March 2006. – Pp. 1260-1266.
8. *Сидельников В.М., Першаков А.С.* Декодирование кодов Рида-Маллера при большом числе ошибок // Пробл. передачи информ. – 1992. – Т.28. - №3. - С.80-94.
9. *Loidreau P., Sakkour B.* Modified version of Sidel'nikov-Pershakov decoding algorithm for binary second order Reed-Muller codes. Ninth International Workshop on Algebraic and Combinatorial Coding theory, ACCT-9. – P.266-271, Kranevo, 2004.
10. *Sakkour B.* Decoding of second order Reed-Muller codes with a large number of errors. ITW2005 - IEEE ITSOC Information Theory Workshop 2005 on Coding and Complexity, Rotoua, New Zealand, 2005.
11. *Деундяк В.М.* Математическое моделирование источников ошибок цифровых каналов передачи данных: учеб. пособие / В.М.Деундяк, Н.С.Могилевская. – Ростов н/Д: Издательский центр ДГТУ, 2006.

Материал поступил в редакцию 21.05.08.

N.S. MOGILEVSKAYA, V.R. SKOROBOGAT, V.S. CHUDAKOV

EXPERIMENTAL RESEARCH OF SECOND ORDER REED-MULLER CODES

In this paper given results of comparative experiments on research of correcting

ability of two Reed-Muller codes likelihood decoders (Sidel’nikov-Pershakov decoder and Loidreau-Sakkour decoder) are presented. For reception of experimental results the program imitating model of the digital data link is realized.

МОГИЛЕВСКАЯ Надежда Сергеевна, доцент кафедры «Программное обеспечение вычислительной техники и автоматизированных систем» ДГТУ, кандидат технических наук. Окончила ДГТУ (2000).
Научные интересы: изучение корректирующих способностей помехоустойчивых кодов по отношению к ошибкам различных типов; моделирование источников ошибок цифровых q-ичных каналов связи.
Автор 30 публикаций.

СКОРОБОГАТ Владимир Романович, (р.1982), аспирант кафедры «Программное обеспечение вычислительной техники и автоматизированных систем» ДГТУ. Окончил ДГТУ (2004) по специальности «Компьютерная безопасность».
Научные интересы: криптографические методы защиты информации; изучение криптоаналитических алгоритмов атак на шифросистемы; применение теории помехоустойчивого кодирования к криптографии.
Автор 7 научных работ.

ЧУДАКОВ Виктор Сергеевич (р.1986). Окончил Донской государственный технический университет по специальности «Компьютерная безопасность».
Научные интересы: помехоустойчивое кодирование, разработка и реализация кодеров/декодеров кода Рида-Маллера различных порядков.
Автор одной научной работы.